LATHAM & WATKINS LLP
Michael H. Rubin (Bar No. 214636)
michael.rubin@lw.com
Melanie M. Blunschi (Bar No. 234264)
melanie.blunschi@lw.com
Francis J. Acott (Bar No. 331813)
francis.acott@lw.com
505 Montgomery St., Suite 2000
San Francisco, CA 94111
Telephone: +1.415.391.0600
Facsimile: +1.415.395.8095

Attorneys for Defendant Amplitude, Inc.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

VIVEK SHAH,

Plaintiff,

v.

AMPLITUDE, INC., a Delaware corporation,

Defendant.

Case No. 2:24-cv-08155-MEMF-JPR

DEFENDANT AMPLITUDE INC.'S NOTICE OF MOTION AND MOTION TO DISMISS COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF

Judge: Maame Ewusi-Mensah Frimpong
Date: April 3, 2025
Time: 10:00 a.m.
Place: Courtroom 8B

NOTICE OF MOTION AND MOTION TO DISMISS

TO THE COURT, ALL PARTIES, AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on April 3, 2025 at 10:00 a.m., or as soon thereafter as the matter can be heard, Defendant Amplitude, Inc. ("Amplitude") will and hereby moves the Court for an order dismissing Plaintiff's Complaint (Dkt. 1).

Amplitude respectfully submits this Motion pursuant to (1) Federal Rule of Civil Procedure ("Rule") 12(b)(1) on the ground that Plaintiff lacks Article III standing because he did not suffer any concrete, particularized harm traceable to Amplitude; and (2) Rule 12(b)(6) on the ground that Plaintiff does not allege facts sufficient to state a violation of (a) the Federal Wiretap Act, 18 U.S.C. § 2510, *et seq.*, (b) the California Invasion of Privacy Act ("CIPA"), Penal Code § 638.51, (c) the California Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Penal Code § 502, or (d) the California Wiretap Act, Penal Code § 631(a).

This Motion is based on the accompanying Memorandum of Points and Authorities, the Declaration of Michael H. Rubin, the Declaration of Brian Cramer, the Declaration of Jeffrey Wang, the pleadings, records, and papers on file, and such argument and evidence as may be presented in connection with the hearing on this Motion.

This Motion is made following the conference of Amplitude's counsel and Plaintiff (who is proceeding *pro se*) pursuant to Local Rule 7-3, which took place on October 16 and 18, 2024.

Dated: October 23, 2024

Respectfully submitted,

LATHAM & WATKINS LLP

By /s/ *Michael H. Rubin*
Michael H. Rubin

Attorneys for Defendant Amplitude, Inc.

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. BACKGROUND 3

A. Amplitude Helps App Developers Such As DoorDash Analyze Their Data 3

B. DoorDash Discloses in Its Privacy Policy That It Shares Personal Information With Service Providers Like Amplitude 3

C. All DoorDash Users Must Consent to its Privacy Policy—including Plaintiff 4

III. ARGUMENT 5

A. Plaintiff Lacks Article III Standing 5

1. Legal Standard 5

2. Plaintiff Consented To DoorDash's Collection And Sharing Of His Information With "Analytics Services" Like Amplitude 6

3. Plaintiff Does Not Allege A Concrete, Particularized Harm Traceable To Amplitude 8

4. Plaintiff Lacks Standing To Pursue Injunctive Relief 11

B. Plaintiff Has Not Stated Any Claim Against Amplitude 11

1. Legal Standard 11

2. Plaintiff Cannot State Any Claim Because He Consented To The Collection And Sharing Of His Information With "Analytics Services" 11

3. Plaintiff Cannot State A Claim For Wiretapping 12

4. Plaintiff's Section 638.51 Claim Should Be Dismissed Because Amplitude's SDK Is Not A Pen Register 18

5. Plaintiff's CDAFA Claim Fails On Multiple Grounds 19

IV. CONCLUSION 21

TABLE OF AUTHORITIES

Page(s)

CASES

Ashcroft v. Iqbal,
556 U.S. 662 (2009) 11

Avilez v. Garland,
69 F.4th 525 (9th Cir. 2023) 10

Bell Atl. Corp. v. Twombly,
550 U.S. 544 (2007) 11

Birdsong v. Apple, Inc.,
590 F.3d 955 (9th Cir. 2009) 5, 9

Byars v. Hot Topic, Inc.,
656 F. Supp. 3d 1051 (C.D. Cal. 2023) 15

Byars v. Sterling Jewelers, Inc.,
2023 WL 2996686 (C.D. Cal. Apr. 5, 2023) 11

Campbell v. Facebook Inc.,
77 F. Supp. 3d 836 (N.D. Cal. 2014) 17

Chapman v. Pier 1 Imports (U.S.) Inc.,
631 F.3d 939 (9th Cir. 2011) 19

Clapper v. Amnesty Int'l USA,
568 U.S. 398 (2013) 11

Cody v. E. Gluck Corp.,
2024 WL 4314187 (N.D. Cal. Sept. 26, 2024) 9

Cottle v. Plaid Inc.,
536 F. Supp. 3d 461 (N.D. Cal. 2021) 20

Doe I v. Google LLC,
2024 WL 3490744 (N.D. Cal. Jul. 22, 2024) 13, 19

Doe v. Google LLC,
2023 WL 6882766 (N.D. Cal. Oct. 18, 2023) 18

Doe v. Kaiser Found. Health Plan, Inc.,
2024 WL 1589982 (N.D. Cal. Apr. 11, 2024) 15

Doe v. Meta Platforms, Inc.,
690 F. Supp. 3d 1064 (N.D. Cal. Sep. 7, 2023) 20

Entropic Commc'ns, LLC v. Comcast Corp.,
702 F. Supp. 3d 954 (C.D. Cal. 2023)... 5

Fish v. Tesla, Inc.,
2022 WL 1552137 (C.D. Cal. May 12, 2022).. 20

Fleming v. ProVest California LLC,
2021 WL 6063565 (N.D. Cal. Dec. 22, 2021) 11

Frasco v. Flo Health, Inc.,
2022 WL 21794391 (N.D. Cal. June 6, 2022) 15

Gonzales v. Uber Techs., Inc.,
305 F. Supp. 3d 1078 (N.D Cal. 2018) 19

Graham v. Noom, Inc.,
533 F. Supp. 3d 823 (N.D. Cal. 2021)...14, 15, 17

Hammerling v. Google LLC,
2022 WL 17365255 (N.D. Cal. Dec. 1, 2022), *aff'd*, 2024 WL 937247 (9th Cir. Mar. 5, 2024) 10

Hammerling v. Google LLC,
615 F. Supp. 3d 1069 (N.D. Cal. 2022) 7, 16, 17

Hammerling v. Google, LLC,
2024 WL 937247 (9th Cir. Mar. 5, 2024) 7

Heeger v. Facebook, Inc.,
509 F. Supp. 3d 1182 (N.D. Cal. 2020) 9

Heiting v. Taro Pharms. USA, Inc.,
2024 WL 1626114 (C.D. Cal. Apr. 2, 2024).. 17

Heiting v. Taro Pharms. USA, Inc.,
709 F. Supp. 3d 1007 (C.D. Cal. 2023)... 17, 19

Hernandez v. Hillsides,
47 Cal. 4th 272 (2009)... 8, 10

I.C. v. Zynga, Inc.,
600 F. Supp. 3d 1034 (N.D. Cal. 2022) 9

In re Facebook, Inc. Internet Tracking Litig.,
956 F.3d 589 (9th Cir. 2020) 5, 11, 14, 20

In re Gilead Scis. Sec. Litig.,
536 F.3d 1049 (9th Cir. 2008) 11

In re iPhone Application Litig.,
844 F. Supp. 2d 1040 (N.D. Cal. 2012) 16

In re Zynga Priv. Litig.,
750 F.3d 1098 (9th Cir. 2014) 16

Ji v. Naver Corp.,
2022 WL 4624898 (N.D. Cal. Sept. 30, 2022) 9

Johnson v. Blue Nile, Inc.,
2021 WL 1312771 (N.D. Cal. Apr. 8, 2021) 14

Jones v. Peloton Interactive, Inc.,
2024 WL 1123237 (S.D. Cal. Mar. 12, 2024) 16, 17

Konop v. Hawaiian Airlines, Inc.,
302 F.3d 868 (9th Cir. 2002) 17

Lau v. Gen Digit. Inc.,
2024 WL 1880161 (N.D. Cal. Apr. 3, 2024) 17

Leite v. Crane Co.,
749 F.3d 1117 (9th Cir. 2014) 5

Licea v. Am. Eagle Outfitters, Inc.,
659 F. Supp. 3d 1072 (C.D. Cal. 2023) 13, 14

Lightoller v. Jetblue Airways Corp.,
2023 WL 3963823 (S.D. Cal. June 12, 2023) 11

M.G. v. Therapy Match, Inc.,
2024 WL 4219992 (N.D. Cal. Sept. 16, 2024) 18

Metzler Inv. GMBH v. Corinthian Colls., Inc.,
540 F.3d 1049 (9th Cir. 2008) 12

Mikulsky v. Noom, Inc , ,
682 F. Supp. 3d 855, 865 (S.D. Cal. 2023 11

NovelPoster v. Javitch Canfield Grp.,
140 F. Supp. 3d 938 (N.D. Cal. 2014)...20

People v. Larkin,
194 Cal. App. 3d 650 (1987)..19

Pratt v. Higgins,
2023 WL 4564551 (N.D. Cal. July 17, 2023)..20

Randall v. United Network for Organ Sharing,
2024 WL 2035828 (C.D. Cal. Mar. 11, 2024)..5

Rodriguez v. Google LLC,
2022 WL 214552 (N.D. Cal. Jan. 25, 2022)...17, 18

Roe v. Amgen Inc.,
2024 WL 2873482 (C.D. Cal. June 5, 2024)...18, 20

Russo v. Microsoft Corp.,
2021 WL 2688850 (N.D. Cal. June 30, 2021)..9

S.D. v. Hytto Ltd.,
2019 WL 8333519 (N.D. Cal. May 15, 2019)..17

Safe Air for Everyone v. Meyer,
373 F.3d 1035 (9th Cir. 2004)...5

Saleh v. Nike, Inc.,
562 F. Supp. 3d 503 (C.D. Cal. 2021)...7

Silver v. Stripe Inc.,
2021 WL 3191752 (N.D. Cal. July 28, 2021)..8

Spreewell v Golden State Warriors,
266 F.3d 979 (9th Cir. 2011)..11

Steckman v. Hart Brewing Inc.,
143 F.3d 1293 (9th Cir. 1998)..12

Summers v. Earth Is. Inst.,
555 U.S. 488 (2009) 11

Swarts v. Home Depot,
689 F. Supp. 3d 732 (N.D. Cal. 2023)........15, 18

Tae Hee Lee v. Toyota Motor Sales, U.S.A., Inc.,
992 F. Supp. 2d 962 (C.D. Cal. 2014)........9

TransUnion LLC v. Ramirez,
590 U.S. 413 (2021) ....passim

United States v. Olson,
856 F.3d 1216 (9th Cir. 2017)........21

Valenzuela v. Keurig Green Mountain, Inc.,
2023 WL 6609351 (N.D. Cal. Oct. 10, 2023)........9

Valenzuela v. Keurig Green Mountain, Inc.,
674 F. Supp. 3d 751 (N.D. Cal. 2023)........14

Vizio Inc. Consumer Priv. Litig.,
238 F. Supp. 3d 1204 (C.D. Cal. 2017)........18

Williams v. What If Holdings, LLC,
2022 WL 17869275 (N.D. Cal. Dec. 22, 2022) 13, 15

Yale v. Clicktale, Inc.,
2021 WL 1428400 (N.D. Cal. Apr. 15, 2021) 14

Yockey v. Salesforce, Inc.,
688 F. Supp. 3d 962 (N.D. Cal. 2023)........15

Yoon v. Lululemon USA, Inc.,
549 F. Supp. 3d 1073 (C.D. Cal. 2021)........16

STATUTES

18 U.S.C. § 2510, *et seq* 1

18 U.S.C. § 2511........15, 25

Cal. Civ. Code § 1798.140 ....8, 20

Cal. Penal Code § 502 ....passim

Cal. Penal Code § 631 ....passim

Cal. Penal Code § 638.50 27

Cal. Penal Code § 638.51 ....2, 3, 15, 26

RULES

Fed. R. Civ. P. 12..passim

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

This is a copycat lawsuit brought by a serial litigant seeking to piggyback on a complaint recently filed in the Northern District of California.[1] Unfortunately for Plaintiff, the complaint that he copied comes from a manufactured dispute with neither the law, the facts, nor common sense on its side.

Plaintiff Vivek Shah—a user of the DoorDash food delivery app and serial litigant—expressly agreed that DoorDash could collect his personal information directly from his device *and* share it with service providers (specifically including analytics services) when he signed up to use the app. He now claims that because he did not provide this consent specifically to Amplitude, Inc. ("Amplitude"), the developer of the specific software development kit ("SDK") that DoorDash embedded in its app, he should be able to bring a raft of wiretapping, hacking and other privacy claims and trigger windfall statutory damages. Make no mistake, Plaintiff alleges nothing more than routine data processing by a service provider. And his radical effort to expand privacy liability and impose it on an entire industry of service providers that simply provide commonly-used software tools (SDKs) to their customers fails for lack of standing and failure to plead elements of each claim.

Plaintiff lacks Article III standing under *TransUnion LLC v. Ramirez*, 590 U.S. 413 (2021). Even crediting that what he alleges actually occurred, none of the conduct could have harmed him—let alone in a concrete, particularized way that is "traditionally recognized" by American courts. *Id.* at 417. Instead, Plaintiff relies solely on a *generalized* claim of privacy harm—which would never suffice for Article III standing—but also fails to meet the high bar for privacy injury, which requires pleading not only a "reasonable expectation of privacy" in the information

[1] *See Atkins v. Amplitude, Inc.*, No. 3:24-cv-04913 (filed Aug. 8, 2024). As detailed in the concurrently-filed Motion to Stay, this action should be stayed pending resolution of the *Atkins* action or, alternatively, transferred to the Northern District of California.

but also that its disclosure constitutes a "highly offensive privacy intrusion." *As a factual matter*, Plaintiff cannot establish either requirement because he agreed to DoorDash's collection and subsequent sharing of his information with analytics services like Amplitude. *As a facial matter*, notwithstanding Plaintiff's artful pleading, his allegations are also deficient: the theoretical ability that Amplitude could receive his delivery address or data about what kind of food he ordered is not a privacy injury.

Even if Plaintiff could meet his burden to establish standing, the Complaint still fails under Rule 12(b)(6) because Plaintiff does not state any claim against Amplitude. Plaintiff asserts causes of action pursuant to the (1) Federal Wiretap Act, 18 U.S.C. § 2510, *et seq.*, (2) the California Wiretap Act, Penal Code § 631(a), (3) California Invasion of Privacy Act ("CIPA"), Penal Code § 638.51, and (4) California Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Penal Code § 502. None is adequately pled as a matter of law.

<u>No Wiretapping</u>: Plaintiff's California and federal wiretapping claims fail. His allegations reflect that Amplitude was acting as an extension of DoorDash, which means Amplitude could not have "eavesdropped" at all. On top of this, Plaintiff's threadbare complaint fails to allege basic elements of a wiretapping claim, including identifying the "content" of his communication or that any content was "intentionally" or "willfully" intercepted "in transit." The federal wiretapping claim fails for the additional reason that one party's consent is a complete defense, and Plaintiff acknowledges that DoorDash consented to share his data with Amplitude.

<u>No Pen Register Under CIPA:</u> Plaintiff's attempt to apply the pen register provision in CIPA § 638.51—which was enacted to regulate law enforcement surveillance—to SDKs would have sweeping consequences on the software industry. But that result need not happen here: this claim is doomed because it was DoorDash, not Amplitude, that installed the SDK in the DoorDash app.

<u>No CDAFA Violation</u>: Plaintiff not only fails to allege the sort of economic

harm from computer damage necessary to meet CDAFA's narrow statutory standing requirements, he does not plausibly allege Amplitude's knowledge that DoorDash supposedly lacked Plaintiff's consent to share his data—no surprise, given DoorDash's readily accessible, publicly available Privacy Policy reflecting that it obtains the consent of its users to share data with analytics services.

II. BACKGROUND

A. Amplitude Helps App Developers Such As DoorDash Analyze Their Data

Amplitude is a data analytics service provider that offers tools to help businesses understand how people use their products. *See* Compl. ¶ 3. One of those tools is a publicly available SDK, prebuilt software that Amplitude's developer customers configure for "their applications to save time and execute specific tasks." *Id.* ¶¶ 14, 20. By using Amplitude's SDK and analytics platform, developers can analyze their own data and learn how users engage with their apps and what product features are successful. Amplitude's SDK is used by thousands of app developers in a broad range of apps—including DoorDash, a popular food delivery app. *Id.* ¶¶ 2, 14, 15. Amplitude's customers install the SDK and configure it for their specific use, including determining what data are processed. *See* Decl. of Jeffrey Wang ("Wang Decl.") ¶ 5.[2] Amplitude does not sell customer data or provide advertising services; it simply provides a platform for businesses to analyze their own data. *Id.* ¶ 7.

B. DoorDash Discloses in Its Privacy Policy That It Shares Personal Information With Service Providers Like Amplitude

Users must agree to DoorDash's Privacy Policy when they sign up for the app. Cramer Decl. ¶¶ 7-10. DoorDash's Privacy Policy expressly discloses that DoorDash collects certain information from users (including through "software

[2] Amplitude concurrently submits the Declarations of Brian Cramer ("Cramer Decl.") and Jeffrey Wang ("Wang Decl") in support of its factual attack on standing under Rule 12(b)(1), and the Declaration of Michael H. Rubin ("Rubin Decl.") in support of its arguments under Rule 12(b)(6).

development kits"), that DoorDash may share that information with "service providers" (including "analytics services"), and that such service providers "may access, store and process your personal information." *Id.*, Ex. A at §§ III, V.[3]

C. All DoorDash Users Must Consent to its Privacy Policy—including Plaintiff

Plaintiff Vivek Shah alleges he is a user of the DoorDash app. Compl. ¶ 32. He alleges that DoorDash embedded Amplitude's SDK into its app and sent his data to Amplitude when he "downloaded and used" the app.[4] *Id.* ¶¶ 32-33. He alleges that DoorDash's use of the SDK in its app "allow[ed]" Amplitude to "collect his timestamped geolocation information, device IDs, device fingerprint data, information about which app(s) he uses on his mobile device, search terms he input into the DoorDash app, the products he placed in his shopping cart, and the restaurants and products he viewed," as well as his name and email address. *Id.* ¶ 33. He does not allege what, if anything, he searched or purchased via the app, or what information he provided to the app.

Though Plaintiff alleges he was not informed that DoorDash's app used Amplitude's SDK and that he did not consent "to Amplitude's data collection practices," *id.*, ¶¶ 5, 21, that is contradicted by documents incorporated into the Complaint and subject to judicial notice: he received detailed disclosures from DoorDash about its collection and sharing of information with analytics services and was required to consent to those practices in order to use DoorDash. *See* Cramer Decl. ¶¶ 7-10; Rubin Decl., Exs. 1–2.

[3] The DoorDash Privacy Policy is accessible in the DoorDash app and on the DoorDash website. *See* Cramer Decl. ¶¶ 3, 9. The current Privacy Policy is publicly available at the following link: https://help.doordash.com/legal/document?type=cx-privacy-policy&region=US&locale=en-US.

[4] While not relied upon for any of its dismissal arguments at this stage, Amplitude notes that Plaintiff mischaracterizes Amplitude's SDK and how DoorDash uses it in the DoorDash app.

III. ARGUMENT

A. Plaintiff Lacks Article III Standing

Plaintiff lacks standing. The factual record establishes that he consented to the conduct that he complains about. And the Complaint does not allege any concrete, particularized harm.

1. Legal Standard

To establish Article III standing, a plaintiff "must demonstrate, among other things, that they suffered a concrete harm," meaning a harm with a "'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts." *TransUnion*, 594 U.S. at 440 (citation omitted). For a privacy harm, a plaintiff must plead that their information was subject to a "reasonable expectation of privacy" and that defendant's access to it constituted a "highly offensive intrusion." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020). That injury must be "particularized" (*i.e.*, plaintiff must personally have experienced it), and plaintiff bears the burden of establishing each element of Article III standing. *Birdsong v. Apple, Inc.*, 590 F.3d 955, 960 (9th Cir. 2009) (citation omitted).

Challenges to a plaintiff's standing can be either "factual" or "facial." *Entropic Commc'ns, LLC v. Comcast Corp.*, 702 F. Supp. 3d 954, 961-62 (C.D. Cal. 2023). A "factual" attack "contests the truth of the plaintiff's factual allegations" by "introducing evidence outside the pleadings," whereas a "facial" attack "asserts that" a complaint's allegations are themselves "insufficient on their face to invoke federal jurisdiction." *Leite v. Crane Co.*, 749 F.3d 1117, 1121 (9th Cir. 2014)) (quoting *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004)). In deciding a factual attack, courts may consider evidence like declarations submitted by the parties, and the party opposing the motion to dismiss has the burden of establishing standing by a preponderance of the evidence. *See Randall v. United Network for Organ Sharing*, 2024 WL 2035828, at *3-4 (C.D. Cal. Mar. 11, 2024).

2. Plaintiff Consented To DoorDash's Collection And Sharing Of His Information With "Analytics Services" Like Amplitude

Plaintiff cannot meet his burden to establish standing based on a privacy harm because he consented to the collection of his information by DoorDash and to DoorDash's sharing of that information with service providers, including "analytics services" like Amplitude. The evidence establishes that (1) DoorDash's disclosures described the data collected and with whom it would be shared, and (2) users like Plaintiff must affirmatively consent to those practices in order to use the app.

First, Plaintiff agreed that DoorDash could collect his personal information, including his "Account and Profile Information," "Activity and Transactions," "Geolocation Information,"[5] and "Device Information." Cramer Decl., Ex. A at § II. These categories cover every type of information he identifies in his Complaint. *Compare* Compl. ¶ 33. Plaintiff further agreed that this information could be "collected automatically from [his] device." Cramer Decl., Ex. A at § III. Thus, Plaintiff had notice of and agreed that the data at issue could be collected by DoorDash.

Second, Plaintiff agreed that DoorDash could provide his personal information to its "service providers and vendors," including "analytics services that help us understand usage of our Services." *Id.* at § V. And, critically, Plaintiff also agreed that DoorDash's service providers "may access, store and process" his personal information. *Id.* Plaintiff's own allegations confirm that Amplitude—an analytics services company—was acting as a service provider in supporting DoorDash's operation of its app. *See* Compl. ¶ 33.[6] Plaintiff thus cannot maintain

[5] Pursuant to the DoorDash Privacy Policy, geolocation information will only be collected if the user "consent[s] by enabl[ing] location services." Cramer Decl., Ex. A at § II. Plaintiff alleges that he did so. Compl. ¶ 33.

[6] Under California's comprehensive privacy law, the California Consumer Privacy Act ("CCPA"), a business may share information with a "service provider" for a "valid business purpose," including for "analytic services." Cal. Civ. Code § 1798.140(e)(5)-(6).

that he had a reasonable expectation of privacy that information he voluntarily provided—which was identified in the Privacy Policy as data that may be collected and shared with "service providers"—would not be shared with service providers like Amplitude for the "specific purpose of" providing analytics services. *Hammerling v. Google, LLC*, 2024 WL 937247, at *3 (9th Cir. Mar. 5, 2024) (no reasonable expectation of privacy where data collection practices were "expressly disclosed"); *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 524 (C.D. Cal. 2021) ("A plaintiff cannot have a reasonable expectation of privacy if she consented to the intrusion."). Nor can Plaintiff maintain that any intrusion was "highly offensive," as courts in this Circuit have held "that data collection and disclosure to third parties that is 'routine commercial behavior' is not a 'highly offensive' intrusion of privacy." *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1090 (N.D. Cal. 2022) (collecting cases). And this case involves nothing more than routine commercial behavior: Amplitude simply provides a platform for businesses like DoorDash to analyze their own data—the *customer* installs the SDK and decides what data are processed, and Amplitude does not sell the data, use it to serve ads, or use personal data for its own purposes. *See* Wang Decl. ¶¶ 5-7.

Plaintiff's assertion that he did not provide his consent to *Amplitude* (as opposed to DoorDash, on behalf of itself and its "service providers") is irrelevant. Plaintiff consented to the *act* of DoorDash sharing his "Personal Information" with its "service providers," including those providing "analytics services that help [DoorDash] understand usage of [its] Services." Cramer Decl., Ex. A at § V. As a result, Plaintiff cannot establish that he had a reasonable expectation of privacy in the collection and sharing of the information at issue, or that such conduct was highly offensive. *Silver v. Stripe Inc.*, 2021 WL 3191752, at *4 (N.D. Cal. July 28, 2021) is on point. There, plaintiffs asserted wiretapping claims based on Instacart's use of a third-party payment service on its website. The court dismissed the claims based on the plaintiffs' consent to Instacart's privacy policy, which disclosed that unnamed "partners" of Instacart may use "various technologies" to collect information like identifiers, demographic and commercial information, geolocation data, and inferences. *Id.*[7]

3. Plaintiff Does Not Allege A Concrete, Particularized Harm Traceable To Amplitude On The Face Of The Complaint

Even setting aside the DoorDash evidence, Plaintiff still would lack standing because he has not plausibly alleged that he personally suffered a concrete injury as a result of Amplitude.

Plaintiff suggests that "consumers" generally suffer some undefined "privacy harm" because Amplitude allegedly receives their "sensitive information" from DoorDash without consent, Compl. ¶¶ 26-28, but he does not link that to any "traditionally recognized" harm. *TransUnion*, 594 U.S. at 432. Though "disclosure of private information, and intrusion upon seclusion" can provide the historical analogue under *TransUnion*, *id.* at 425, Plaintiff fails to plead facts supporting such an injury: he does not identify any category of information that he personally shared in which he had a "reasonable expectation of privacy," much less that DoorDash's sharing that information with Amplitude was "highly offensive." *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (2009). The Complaint simply lists a handful of data fields that the Amplitude SDK is *capable* of receiving based on how a person uses the DoorDash app and what DoorDash chooses to send to Amplitude—without any facts about Plaintiff's actual use of the app, what specific information he provided to DoorDash, or why that information is sensitive.[8] For example, Plaintiff alleges that Amplitude collects information about a DoorDash user's search terms,

[7] Although the court's § 631 dismissal was pursuant to Rule 12(b)(6), its reasoning applies here.

[8] Plaintiff's speculation that a hypothetical consumer's geolocation information for their food deliveries *could* reveal their "religious affiliation, sexual orientation, [or] medical condition" is too far-fetched to countenance. Compl. ¶ 26. In any event, he does not allege that his data *actually* reveals such information. *See Birdsong*, 590 F.3d at 960.

shopping cart, and restaurants they viewed, Compl. ¶ 33, but he does not allege that he even used the app's search function, added items to his cart, or placed an order. *See Tae Hee Lee v. Toyota Motor Sales, U.S.A., Inc.*, 992 F. Supp. 2d 962, 972 (C.D. Cal. 2014) (no standing where plaintiffs did not allege "any negative experience" with challenged product feature); *Cody v. E. Gluck Corp.*, 2024 WL 4314187, at *2 (N.D. Cal. Sept. 26, 2024) (no standing where plaintiff did not allege that "she actually used the chat feature"); *Valenzuela v. Keurig Green Mountain, Inc.*, 2023 WL 6609351, at *2 (N.D. Cal. Oct. 10, 2023 (same, where plaintiff did not allege "the contents" of communications with website); *Russo v. Microsoft Corp.*, 2021 WL 2688850, at *3 (N.D. Cal. June 30, 2021) (same, where plaintiffs did not allege that they used certain product features).

Even if Plaintiff had shared all of the data with DoorDash that he identifies, he still could not plausibly allege that disclosure of such information was "highly intrusive." The notion that information about a person adding sushi to their shopping cart or searching for "tacos" resembles a harm "traditionally recognized" by American courts is simply not plausible. *TransUnion*, 594 U.S. at 425. And court after court has recognized that data about a user's device, such as "device IDs", so-called "device fingerprint data" (defined by Plaintiff as "device make and model, screen resolution, and operating system version"), and the like, *see* Compl. ¶¶ 16, 33, are not categories of information that give rise to a cognizable privacy injury. *See, e.g.*, *Ji v. Naver Corp.*, 2022 WL 4624898, at *7 (N.D. Cal. Sept. 30, 2022) (device ID, IP address, operating system data); *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1049-50 (N.D. Cal. 2022) (email address, phone number, username); *Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1189 (N.D. Cal. 2020) (IP address).

The circumstances here make clear that the sharing of data by DoorDash with Amplitude could not be so "'sufficiently serious' and unwarranted as to constitute an 'egregious breach of the social norms'"—as Plaintiff must plead to establish a "highly offensive" intrusion. *Hernandez*, 47 Cal. 4th at 295. This case is about a "food delivery app" analyzing its own app-usage data with tools developed by an analytics company. Compl. ¶ 20. Plaintiff alleges nothing more than routine data processing by a service provider. *See, e.g.*, *Hammerling v. Google LLC*, 2022 WL 17365255, at *9 (N.D. Cal. Dec. 1, 2022), *aff'd*, 2024 WL 937247 (9th Cir. Mar. 5, 2024) (searches for foot massager, slippers, meal subscriptions, coconut oil, and use of photo editor were "data collection of 'routine commercial behavior,'" not highly offensive). And the very data collection and sharing practices that Plaintiff complains about were publicly disclosed in DoorDash's Privacy Policy. *See* Cramer Decl., Ex. A at § V; Rubin Decl., Exs. 1-2. Without an intrusion into his protectable privacy interest, Plaintiff has *at most* alleged a "bare procedural violation[], divorced from any concrete harm," which is insufficient. *TransUnion*, 594 U.S. at 440 (citation omitted).

Nor can Plaintiff argue that an alleged statutory violation alone is somehow a concrete injury. "[A]n injury in law is not an injury in fact." *Id.* at 427 (plaintiff does not "automatically satisf[y] the injury-in-fact requirement whenever a statute grants [him] a statutory right"). Rather, Article III requires a concrete injury "traditionally recognized" by American courts, *id.* at 440, which for disclosure of private information requires a "reasonable expectation of privacy" and a "highly offensive" intrusion.[9] *Hernandez*, 47 Cal. 4th at 286. Plaintiff has alleged nothing of the sort.

[9] To the extent pre-*TransUnion* case law suggested that a statutory violation of certain CIPA provisions could by itself constitute a cognizable harm for standing purposes, that is "clearly irreconcilable," *Avilez v. Garland*, 69 F.4th 525, 533 (9th Cir. 2023), with the Supreme Court's later decision in *TransUnion*. *Compare TransUnion*, 594 U.S. at 426 ("[E]ven though 'Congress may 'elevate' harms that 'exist' in the real world before Congress recognized them to actionable legal status, it may not simply enact an injury into existence, using its lawmaking power to transform something that is not remotely harmful into something that is.'") (citations omitted), *with In re Facebook Internet Tracking*, 956 F.3d at 598-99 (pre-*TransUnion* decision finding standing because of alleged violations of statutory provisions codifying right to privacy). *See also Lightoller v. Jetblue Airways Corp.*, 2023 WL 3963823, at *3 (S.D. Cal. June 12, 2023) (holding that *In re Facebook Internet Tracking*'s holding is "untenable" in light of *TransUnion*); *Fleming v. ProVest California LLC*, 2021 WL 6063565, at *2 (N.D. Cal. Dec. 22, 2021) (holding that "*TransUnion* likely alters the Ninth Circuit standing framework"); *Byars v. Sterling Jewelers, Inc.*, 2023 WL 2996686, at *3 (C.D. Cal. Apr. 5, 2023)

4. Plaintiff Lacks Standing To Pursue Injunctive Relief

Plaintiff also lacks standing to seek injunctive relief (Compl. ¶¶ 48, 55, 64), which requires a threat of "actual and imminent, not conjectural or hypothetical" injury. *Summers v. Earth Is. Inst.*, 555 U.S. 488, 493 (2009). The "threatened injury must be certainly impending." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013) (quotation and alteration omitted). Plaintiff does not allege any future harm whatsoever. Nor could he, since the data collection and sharing practices he complains about are publicly disclosed in DoorDash's Privacy Policy. *See* Cramer Decl. ¶¶ 7-10; Rubin Decl., Exs. 1-2. And he is free to uninstall the DoorDash app.

B. Plaintiff Has Not Stated Any Claim Against Amplitude

1. Legal Standard

"To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A plaintiff must provide "more than labels and conclusions," *Twombly*, 550 U.S. at 555, and the Court need not "accept as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences," *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (quoting *Spreewell v Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2011)).

2. Plaintiff Cannot State Any Claim Because He Consented To The Collection And Sharing Of His Information With "Analytics Services"

All of Plaintiff's claims fail for the threshold reason that he consented to DoorDash's collection of his personal information and the sharing of that information with "service providers," including "analytics services" like Amplitude.

(distinguishing *In re Facebook Internet Tracking* and holding that "bare violation of CIPA" is insufficient for standing); *Mikulsky v. Noom, Inc.*, 682 F. Supp. 3d 855, 865 (S.D. Cal. 2023) (similar).

Each statute at issue here precludes liability where a plaintiff consented. *See* Cal. Penal Code § 631(a) ("without the consent of all parties"), § 638.51 (no violation "[i]f the consent of the user … has been obtained"), § 502(c) ("without permission"), 18 U.S.C. § 2511(2)(d) (no violation if "prior consent"). Though Plaintiff asserts that he did not separately consent to *Amplitude*, *see* Compl. ¶¶ 34-35, he does ***not*** claim that he did not consent to DoorDash. Nor could he: Plaintiff alleges that he "downloaded and used" the DoorDash app, *id.* ¶ 32, which discloses and requires agreement to DoorDash's public Privacy Policy. *See* Rubin Decl., Exs. 1-2.[10] And the DoorDash Privacy Policy clearly discloses that information could be collected and shared with "analytics services," Cramer Decl., Ex. A at § V, defeating all of Plaintiff's claims.

3. Plaintiff Cannot State A Claim For Wiretapping

Plaintiff cannot state a wiretapping claim under CIPA or federal law because he does not plausibly allege that Amplitude intentionally or willfully made an unauthorized connection with his device or intercepted the contents of his communications in transit.

a. Plaintiff Does Not Allege That Amplitude Wiretapped His Phone Or Eavesdropped On His Communications Under CIPA

Plaintiff's CIPA claim is entirely conclusory: he simply quotes § 631(a) and declares that Amplitude's SDK "made an unauthorized connection" with his device and "intercepted" his "input events" (Compl. ¶¶ 58-59) without any facts or

[10] DoorDash's Privacy Policy, the sign-up and login screen, and the sign up page are incorporated by reference and judicially noticeable, as detailed in the concurrently-filed Request for Judicial Notice, and thus the Court may consider them in ruling on Amplitude's facial standing and Rule 12(b)(6) challenges. *See Metzler Inv. GMBH v. Corinthian Colls., Inc.*, 540 F.3d 1049, 1061, 1064 n.7 (9th Cir. 2008). The Court need not "accept as true conclusory allegations which are contradicted by documents referred to in the complaint." *Steckman v. Hart Brewing Inc.*, 143 F.3d 1293, 1295–96 (9th Cir. 1998).

explanation. Based on his vague references to an "unauthorized connection" and "intercept[ion],"[11] Plaintiff appears to assert claims under the first two clauses of § 631(a), which respectively prohibit (1) "intentionally" making an "unauthorized connection" with any "telegraph or telephone wire, line, cable, or instrument" (*i.e.*, intentional wiretapping), and (2) "willfully attempting to learn the contents or meaning" of a communication "in transit" (*i.e.*, eavesdropping). Cal. Penal Code § 631(a). Both fail.

First, as a threshold matter, Plaintiff fails to sufficiently plead either claim because the Complaint lacks facts indicating that Amplitude engaged in any "willful or intentional conduct," as required to state a claim under § 631(a). *See* Cal. Penal Code § 631; *Doe I v. Google LLC*, 2024 WL 3490744, at *6 (N.D. Cal. Jul. 22, 2024) ("CIPA liability only extends to willful or intentional conduct."). Plaintiff alleges that DoorDash, not Amplitude, embedded the SDK in the DoorDash app, and there are no factual allegations suggesting that Amplitude expected DoorDash to share data from users who were not on notice of DoorDash's data collection practices. *See Doe I*, 2024 WL 3490744, at *6.

Second, as a matter of law, Plaintiff cannot state a claim for making "an unauthorized connection" with his device. That provision in § 631(a) does not cover internet communications, even when made using a smartphone. *See Licea v. Am. Eagle Outfitters, Inc.*, 659 F. Supp. 3d 1072, 1079 (C.D. Cal. 2023) ("Courts have consistently interpreted this clause [of § 631(a)] as applying only to communications over telephones and not through the internet."); *see also Valenzuela v. Keurig Green Mountain, Inc.*, 674 F. Supp. 3d 751, 755 (N.D. Cal. 2023). Because Plaintiff does not allege that Amplitude's SDK operates using telegraph or telephone wires (nor could he), he fails to state a wiretapping claim under the first clause of

[11] Courts construe references to "interception" as invoking the second clause of § 631(a). *See, e.g.*, *Williams v. What If Holdings, LLC*, 2022 WL 17869275, at *2 (N.D. Cal. Dec. 22, 2022).

§ 631(a).

Third, Plaintiff fails to plead essential elements of a claim for intercepting communications. The Complaint alleges that Amplitude was acting as an authorized extension of DoorDash and thus is exempted under § 631(a), and Plaintiff has not alleged, as he must to state a claim, the "contents" of the allegedly intercepted communication or that it was intercepted while "in transit."

No Eavesdropping. Section 631 exempts any "'party' to the communication." *In re Facebook Internet Tracking*, 956 F.3d at 607. Courts have applied this exemption to third-party service providers where, as here, the allegations indicate that the provider was acting merely as an extension of a party. *See, e.g.*, *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823 (N.D. Cal. 2021) (vendor providing session replay software to record website activity was extension of website operator); *Johnson v. Blue Nile, Inc.*, 2021 WL 1312771, at *1 (N.D. Cal. Apr. 8, 2021) (same); *Yale v. Clicktale, Inc.*, 2021 WL 1428400, at *1, *3 (N.D. Cal. Apr. 15, 2021) (similar); *Licea*, 659 F. Supp. 3d at 1083 (citing *Graham*, 533 F. Supp. 3d at 833, and reaching same conclusion).

Here, Plaintiff's allegations reflect that Amplitude was acting as an authorized extension of DoorDash. Plaintiff alleges that developers like DoorDash "integrate" the SDK into their apps "to save time and execute specific tasks." Compl. ¶¶ 3, 14, 20. Though the Complaint tries to obfuscate Amplitude's role as a service provider by asserting that Amplitude "collects" the data (*e.g.*, *id.* ¶¶ 13, 20), the totality of Plaintiff's allegations—and the agreements he consented to—show that Amplitude received the information after Doordash collected it and that Amplitude was performing functions *for* DoorDash. And simply "provid[ing] a tool" that "allows [a business] to record and analyze its own data" does not make a service provider an eavesdropper.[12] *Graham*, 533 F. Supp. 3d at 832 (vendor provided software that

[12] Notably, the CCPA defines a "third party" as a "person who is *not* … a service provider to the business." Cal. Civ. Code § 1798.140(ai) (emphasis added).

captured "clients' data" and allowed client to analyze it) (citation omitted); *Yockey v. Salesforce, Inc.*, 688 F. Supp. 3d 962, 973 (N.D. Cal. 2023) (no allegation that vendor used data for other purposes); *Williams*, 2022 WL 17869275, at *3 (distinguishing vendors that use client data for separate business purposes).

In an attempt to plead around the party exception, the Complaint includes two vague paragraphs nodding to supposed "integrations" with advertising platforms and the development of "artificial intelligence tools to analyze the data," Compl. ¶¶ 29-30, but these allegations are entirely conclusory and untethered to the DoorDash app and to Plaintiff's data. They are also insufficient to transform Amplitude from a service provider to an eavesdropper. Whether a vendor functions as an extension of its business customer hinges on whether the business has the "control and ability to limit" dissemination of the data, *Doe v. Kaiser Found. Health Plan, Inc.*, 2024 WL 1589982, at *18 (N.D. Cal. Apr. 11, 2024), and courts typically look to whether the vendor resells the data or uses it for advertising. *See Swarts v. Home Depot*, 689 F. Supp. 3d 732, 746 (N.D. Cal. 2023) (no allegation that analytics provider could use information "for any other purpose besides relaying it to [customer]"); *Graham*, 533 F. Supp. 3d at 832 (distinguishing software vendors providing "tools" from "independent parties who mined information from other websites and sold it"); *Byars v. Hot Topic, Inc.*, 656 F. Supp. 3d 1051, 1068 (C.D. Cal. 2023) (vendor was extension of party where there was no allegation that vendor aggregated data for resale); *see also Frasco v. Flo Health, Inc.*, 2022 WL 21794391, at *1 (N.D. Cal. June 6, 2022) (no factual allegation about service provider "us[ing] the data provided to it through its SDK for '[its] own purposes'"). Here, Plaintiff merely alleges that Amplitude "created integrations" for its customers to share their own data "with marketing and advertising platforms," Compl. ¶ 29—***not*** that Amplitude itself sells data or uses it in an advertising business that it runs. (Amplitude does not sell data and has no ad business.)

No "Content" at Issue. Plaintiff's claim under this subsection additionally fails because he has not alleged the "contents or meaning" of any intercepted communication. *Jones v. Peloton Interactive, Inc.*, 2024 WL 1123237, at *4 (S.D. Cal. Mar. 12, 2024) (conclusory allegation that vendor captured transcript of online chat failed to plead "content"). Under CIPA, the "contents" of a communication are limited to "the intended message conveyed by the communication." *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). Indeed, the Complaint lacks any factual allegations about the "intended message" of *any* communication whatsoever.

Plaintiff's theory is that the SDK intercepted his "specific input events," *i.e.*, page views, button presses, or other "affirmative actions (such as installing a mobile app on his device)." Compl. ¶ 58. But this information does not reveal any message that Plaintiff intended to convey to DoorDash. This information is "automatically generated" and "does not comprise the substance, purport, or meaning of that communication." *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012). Courts have dismissed eavesdropping claims based on similar information. *See Jones*, 2024 WL 1123237, at *4 ("IP address, device used to connect to website, web browser used, date and time of communication, [and] words used to prompt the chat" are not content); *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1082 (C.D. Cal. 2021) (distinguishing non-content like "keystrokes, mouse clicks, pages viewed, and shipping and billing information" from content like "words of a text message"); *see also Hammerling*, 615 F. Supp. 3d at 1093 ("habits and identities" inferred from apps not "content").[13]

Plaintiff's generic reference to the collection of "search terms" cannot save him. Because Plaintiff does not even identify a search term he used (if any), he

[13] Even if Plaintiff could assert an "unauthorized connection" claim (he cannot), the information underlying that claim (Compl. ¶ 59) is not "content" because it relates to device settings and it is automatically generated "record information." *Graham*, 533 F. Supp. 3d at 833 (citation omitted); *S.D. v. Hytto Ltd.*, 2019 WL 8333519, at *6 (N.D. Cal. May 15, 2019).

necessarily fails to plead the existence of any "content." *Jones*, 2024 WL 1123237, at *4; *Heiting v. Taro Pharms. USA, Inc.*, 709 F. Supp. 3d 1007, 1018 (C.D. Cal. 2023). In any event, determining whether search terms qualify as "content" requires a "case-specific analysis" that turns on "how much information would be revealed" by disclosure. *Hammerling*, 615 F. Supp. 3d at 1092. Here, Plaintiff cannot plausibly allege that his searches for food items were protected content.

No Allegations About Communications "In Transit." Plaintiff also fails to allege, as he must, that his communications were "stop[ped], seize[d], or interrupt[ed] in progress or course before arrival." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002); *Lau v. Gen Digit. Inc.*, 2024 WL 1880161, at *1 (N.D. Cal. Apr. 3, 2024) ("The wiretapping statutes … are directed at the unauthorized interception of communications, not any subsequent storage and/or use."). Plaintiff cannot meet his pleading burden by simply using the word "interception," which is all he did in the Complaint. Compl. ¶ 25. He must allege facts "regarding the method, or nature, of interception" that occurred. *Heiting v. Taro Pharms. USA, Inc.*, 2024 WL 1626114, at *9 (C.D. Cal. Apr. 2, 2024) (citing *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 848 (N.D. Cal. 2014)). Similarly, Plaintiff's claim that the SDK collects information "intended for the mobile app" "in real-time" (Compl. ¶ 19) fails to allege that Amplitude accessed *his* data *before* it supposedly reached the app. Courts throughout California have rejected vague allegations like those here. *See, e.g.*, *Lau*, 2024 WL 1880161, at *1 (allegation that defendant "catalogued and stored" data); *Rodriguez v. Google LLC*, 2022 WL 214552, at *1-2 (N.D. Cal. Jan. 25, 2022) (references to communications being "intercepted" and "simultaneous"); *Swarts*, 689 F. Supp. 3d at 746 (similar); *Vizio Inc. Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1228 (C.D. Cal. 2017) (similar).

b. Plaintiff Alleges That DoorDash Consented To The Use Of Amplitude's SDK, Barring His Federal Wiretapping Claim

Plaintiff's federal wiretapping claim fails for all the same reasons as his California claim—and more. *See supra* Section III.B.3.a; *M.G. v. Therapy Match, Inc.*, 2024 WL 4219992, at *3 (N.D. Cal. Sept. 16, 2024) (analysis for CIPA the same as federal Wiretap Act). Unlike CIPA, the Federal Wiretap Act is a one-party consent statute and one party's consent is a complete defense. *See* 18 U.S.C. § 2511(2)(d). DoorDash consented to the use of Amplitude's SDK by installing it in its app. Plaintiff's own allegations indicate that DoorDash *chose* to "embed[]" the SDK in its app (Compl. ¶ 33), which is fatal. Courts routinely dismiss federal wiretapping claims on this basis. *See, e.g.*, *Doe v. Google LLC*, 2023 WL 6882766, at *2 (N.D. Cal. Oct. 18, 2023); *Rodriguez*, 2021 WL 2026726, at *6; *Roe v. Amgen Inc.*, 2024 WL 2873482, at *6 (C.D. Cal. June 5, 2024).

4. Plaintiff's Section 638.51 Claim Should Be Dismissed Because Amplitude's SDK Is Not A Pen Register

Plaintiff seeks to upend the software industry's reliance on SDKs by asserting that Amplitude is liable because its SDK—which Doordash integrated in its own app—is a "pen register" used to track his information under § 638.51. Compl. ¶ 46. This claim fails.

First, Plaintiff does not allege that Amplitude "install[ed] or use[d]" the SDK, as required. Cal. Penal Code § 638.51(a). To the contrary, he alleges that *DoorDash* "embedded" the SDK in its own app and that the SDK was used by that app to collect data. Compl. ¶¶ 20, 33.

Second, Plaintiff does not allege that the SDK is a pen register, which has a very specific meaning: it is "a device or process that records or decodes dialing, routing, addressing, or signaling information . . . ." § 638.50(b). Rather than plead facts, the Complaint simply parrots the statutory language, claiming the SDK is a "pen register" because it is a "device or process that records addressing or signaling information." Compl. ¶ 46. That is circular and entirely conclusory. *See Chapman v. Pier 1 Imports (U.S.) Inc.*, 631 F.3d 939, 955 n.9 (9th Cir. 2011) (plaintiff must do more than "parrot" statutory language). In any event, Plaintiff alleges that app developers like DoorDash "integrate SDKs into their apps to save time and execute specific tasks," and that the SDK *collects* information from a device, Compl. ¶ 14—which is nothing like a pen register.[14]

5. Plaintiff's CDAFA Claim Fails On Multiple Grounds

Plaintiff's CDAFA claim fares no better: on top of being entirely conclusory, it fails for lack of statutory standing because Plaintiff does not allege any economic damages related to damage to his device and because Plaintiff has not pled that Amplitude knew that DoorDash was sending data to Amplitude without permission—nor can he. *See* Cal. Penal Code § 502(a), (e).

Parroting the Statute Is Not Enough. The CDAFA prohibits the "tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a). Plaintiff invokes three subsections of the CDAFA, but merely parrots the language of the statute. That alone warrants dismissal. *See Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1090 (N.D Cal. 2018) (dismissing "boilerplate" claim).

No Cognizable Loss. Plaintiff lacks statutory standing to bring a CDAFA claim, which requires "damage or loss by reason of a violation" of the statute. Cal. Penal Code § 502(e); *Doe I*, 2024 WL 3490744, at *8; *Heiting v. Taro Pharms. USA, Inc.*, 709 F. Supp. 3d 1007, 1020 (C.D. Cal. 2023) (collecting cases).[15] Courts

[14] Amplitude disputes that § 638.51 applies to the software alleged here, or that a pen register encompasses technology that captures the originating information of an outbound communication, *see People v. Larkin*, 194 Cal. App. 3d 650, 653 n.2 (1987), but reserves these arguments in light of recent decisions in this Circuit.

[15] Courts typically apply the definitions of "damage" and "loss" from the federal Computer Fraud and Abuse Act ("CFAA") to the CDAFA. *See NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 951 (N.D. Cal. 2014) (no damage or loss under CDAFA "for the same reason" as CFAA).

narrowly construe "loss" under the CDAFA, "to encompass costs related to fixing a computer, lost revenue, or other consequential damages incurred due to an interruption of computer services." *Pratt v. Higgins*, 2023 WL 4564551, at *9 (N.D. Cal. July 17, 2023) (improper access to medical information not a loss); *Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1081 (N.D. Cal. Sep. 7, 2023) (privacy violation not loss); *Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461, 488 (N.D. Cal. 2021) (excluding "'right to control [one's] own data, the loss of the value of their data, and the loss of the right to protection of the data" from "damage or loss").

Plaintiff does not even attempt to identify any damage to his device from the use of the SDK in the DoorDash app, much less costs to fix it or consequential damages suffered as a result. *See* Compl. ¶¶ 49-55. That should end the inquiry here. *See Fish v. Tesla, Inc.*, 2022 WL 1552137, at *8 (C.D. Cal. May 12, 2022) (dismissing CFAA claim). Instead, Plaintiff alleges that Amplitude "was unjustly enriched with the data it obtained" from him. Compl. ¶ 54. This theory appears to be based on *In re Facebook Internet Tracking*, an outlier case where the CDAFA loss allegations were based on plaintiffs' claim to profits from the unauthorized sale of their browsing histories for advertising. 956 F.3d at 600. But there, the defendant was alleged to have earned revenue directly from the sale of the plaintiffs' data, bringing the allegations within the ambit of "lost revenue" given that plaintiffs alleged a market for their data. Here, in contrast, there is no allegation (nor could Plaintiff make one in good faith) that Amplitude sold Plaintiff's data or used it for advertising. Nor does Plaintiff allege that there is a market for his DoorDash data. Put simply, Plaintiff has not alleged any facts showing that Amplitude was unjustly enriched. *See Amgen Inc.*, 2024 WL 2873482, at *7 (dismissing claim without allegation that defendant "sold [plaintiffs'] data" or how defendant was unjustly enriched).

No Allegation Regarding Amplitude's Knowledge. Plaintiff's claim also fails because he does not allege that Amplitude "knowingly" received his data "without permission."[16] Cal. Penal Code §§ 502(c)(1)-(2), (c)(7). The Complaint is silent as to Amplitude's knowledge and does not even suggest that it knew DoorDash lacked permission to share Plaintiff's data—not surprising, given DoorDash's public Privacy Policy disclosing that information may be shared with analytics services.

IV. CONCLUSION

For the foregoing reasons, Amplitude respectfully requests dismissal of the Complaint.

Dated: October 23, 2024

Respectfully submitted,

LATHAM & WATKINS LLP

By /s/ *Michael H. Rubin*
Michael H. Rubin

Attorneys for Defendant Amplitude, Inc

CERTIFICATE OF COMPLIANCE

The undersigned, counsel of record for Defendant Amplitude, Inc., certifies that this brief contains 21 pages, which complies with page limit set by the Court's May 3, 2024 Civil Standing Order.

[16] CDAFA is a criminal statute, and "[a]bsent indication of contrary purpose in the language or legislative history [], [courts] ordinarily read a phrase in a criminal statute that introduces the elements of a crime with the word 'knowingly' as applying that word to each element." *United States v. Olson*, 856 F.3d 1216, 1220 (9th Cir. 2017). Thus, to state a CDAFA claim, Plaintiff must not only allege that Amplitude lacked permission, but that it *knew* it lacked permission. *Id.*